ABSTRACT

A key agreement method for secure communication in a multiple access system is provided.

A key agreement method for secure communication in a multiple access system, the key agreement method includes the steps of (a) a first user, modulating signals from a source by a bit sequence and transmitting the modulated signal, (b) a second user, a legitimate counterpart of the first user, decoding, making decision for each bit of the signal with a detector affected by noise and recording the measured values, (c) the second user, deciding a threshold value of measurement with consideration of other factors such as a transmission rate, tolerable error rates, and a degree of security, (d) the second user adopting as a key string only bits having values beyond the threshold value and ignoring bits falling the erroneous region below the threshold, (e) the second user informing the first user that the n-th bit is adopted, not telling the value of the bit, and (f) the users, the first user and the second user, taking as a key string the values of the n-th bits adopted in (e), and discarding the values of the other bits.